Claims:

1. A method to manage secure connections, comprising:

receiving an encrypted packet having an identifier and an external address that represents a plurality of internal addresses;

selecting one of said internal addresses; and

communicating said encrypted packet to said selected internal address.

2. The method of claim 1, wherein said selecting comprises:

searching a list of identifiers having associated times;

selecting an identifier having an earliest time; and

retrieving said internal address associated with said selected identifier.

3. The method of claim 2, wherein said searching comprises:

creating said list; and

searching said created list.

4. The method of claim 3, wherein said creating comprises:

receiving an encrypted packet having a predetermined sequence number and an identifier from a device associated with one of said internal addresses;

determining a time said encrypted packet was received;

associating said time and said internal address with said identifier; and

storing said identifier with said associated time and associated internal address.

5. The method of claim 1, wherein said packet is encrypted in accordance with the Internet Security Association And Key Management Protocol (ISAKMP).

6. The method of claim 1, wherein said encrypted packet is an Internet Protocol (IP) Encapsulating Security Payload (ESP) encrypted packet.

7. The method of claim 1, wherein said identifier is a security parameter index (SPI).

8. The method of claim 1, wherein said identifier represents a tunnel between two devices, and further comprising:

receiving a message that said encrypted packet was communicated to an incorrect internal address;

determining activity levels for each tunnel terminating at each device represented by said plurality of internal addresses; and

communicating said encrypted packet to an internal address having a tunnel with a highest activity level.

9. A method to manage secure connections, comprising:

creating a list of identifiers, with each identifier representing a tunnel terminating at a device having an internal address;

translating each of said internal addresses to an external address;

receiving an encrypted packet having said external address;

selecting one of said internal addresses using said list of identifiers; and

communicating said encrypted packet to said selected internal address.

10. The method of claim 9, wherein said tunnel is created in accordance with the Internet Security Association And Key Management Protocol (ISAKMP).

11. The method of claim 9, wherein said encrypted packet is an Internet Protocol (IP) Encapsulating Security Payload (ESP) encrypted packet.

12. The method of claim 9, wherein said identifier is a security parameter index (SPI).

13. The method of claim 9, wherein said selecting comprises:

searching said list of identifiers having associated times;

selecting an identifier having an earliest time; and

retrieving said internal address associated with said selected identifier.

14. The method of claim 9, wherein said creating comprises:

receiving an encrypted packet having an identifier from a device associated with one of said internal addresses;

determining a time said encrypted packet was received;

associating said time and said internal address with said identifier; and

storing said identifier with said associated time and internal destination address.

15. A secure connection manager, comprising:

a flow module to create a list of identifiers, with each identifier representing a secure flow terminating at a device with an internal address; and

a translation module to select an internal address for an encrypted packet having an external address and a flow identifier.

16. The secure connection manager of claim 15, further comprising:

a communication module to communicate said encrypted packet to said selected internal address.

17. A system to manage secure connections, comprising:

a first network node to send encrypted packets to an external address;

a second network node to receive said encrypted packets and translate said external address to an internal address; and

a third network node having said internal address to receive said encrypted packets.

18. The system of claim 17, wherein said second network node is a router configured to perform natural address translation (NAT).

19. The system of claim 17, wherein said first and third network nodes are configured to communicate using a tunnel created in accordance with the Internet Security Association And Key Management Protocol (ISAKMP).

20. The system of claim 17, wherein said encrypted packets are Internet Protocol (IP) Encapsulating Security Payload (ESP) encrypted packets.

21. The system of claim 17, wherein said second network node performs said translation using a list of flow identifiers, with each flow identifier representing a security parameter index (SPI) and having an associated internal address and receipt time.

22. An article comprising:

a storage medium;

said storage medium including stored instructions that, when executed by a processor, result in managing a secure connection by receiving an encrypted packet having an identifier and an external address that represents a plurality of internal addresses, selecting one of said internal addresses, and communicating said encrypted packet to said selected internal address.

23. The article of claim 22, wherein the stored instructions, when executed by a processor, further result in selecting one of said internal addresses by searching a list of identifiers having associated times, selecting an identifier having an earliest time, and retrieving said internal address associated with said selected identifier.

24. The article of claim 23, wherein the stored instructions, when executed by a processor, further result in searching said list of identifiers by creating said list, and searching said created list.

25. The article of claim 24, wherein the stored instructions, when executed by a processor, further result in creating said list by receiving an encrypted packet having a predetermined sequence number and an identifier from a device associated with one of said internal addresses, determining a time said encrypted packet was received, associating said time and said internal address with said identifier, and storing said identifier with said associated time and associated internal address.

26. An article comprising:

a storage medium;

said storage medium including stored instructions that, when executed by a processor, result in managing secure connections by creating a list of identifiers, with each identifier representing a tunnel terminating at a device having an internal address, translating each of said internal addresses to an external address, receiving an encrypted packet having said external address, selecting one of said internal addresses using said list of identifiers, and communicating said encrypted packet to said selected internal address.

27. The article of claim 26, wherein the stored instructions, when executed by a processor, further result in selecting one of said internal addresses by searching said list

of identifiers having associated times, selecting an identifier having an earliest time, and retrieving said internal address associated with said selected identifier.

28. The article of claim 26, wherein the stored instructions, when executed by a processor, further result in creating said list of identifiers by receiving an encrypted packet having an identifier from a device associated with one of said internal addresses, determining a time said encrypted packet was received, associating said time and said internal address with said identifier, and storing said identifier with said associated time and internal destination address.